VZCZCXYZ0000
RR RUEHWEB

DE RUEHKO #1764/01 2150619
ZNY CCCCC ZZH
R 030619Z AUG 09
FM AMEMBASSY TOKYO
TO RHMFISS/DEPT OF HOMELAND SECURITY WASHINGTON DC
RUEHC/SECSTATE WASHDC 5088

C O N F I D E N T I A L TOKYO 001764

SIPDIS

FOR S/CT FOR HILLARY BATJER JOHNSON AND PAUL SCHULTZ, NCTC,
AND DHS

E.O. 12958: DECL: 08/03/2019
TAGS: KVPR PTER PREL PGOV CVIS ASEC KHLS
SUBJECT: RESPONSE TO REQUEST FOR UPDATES ON INFORMATION ON
HOST GOVERNMENT PRACTICES-INFORMATION COLLECTION, SCREENTNG
AND SHARING

REF: A. (A)06 STATE 190832
¶B. (B)07 STATE 133921
¶C. (C)08 STATE 048 120
¶D. (D) STATE 32287

Classified By: CDA James Zumwalt. Reasons: 1.4(b, d)

¶1. (SBU) Immigration Data Bases and Traveler Information
Collection: -- What computerized immigration databases are
used to track entries and exits?

The Immigration Bureau tracks entries and exits for all
travelers, both foreign and Japanese, on a nationwide
computerized database. The system records name, passport
number, date of birth, citizenship, and fight number.
Records of immigration entries and exits are updated
immediately. Primary storage for records on Japanese
travelers is on a host located at Narita International
Airport with backup located at Kasai International Airport.
Primary storage for immigration records for foreigners is
located on a host at Kansai with backup at Narita. -- Is the
computerized immigration database available at all ports of
entry (POEs)?

All ports of entry in Japan, with the possible exception of
some isolated seaports with low vessel traffic, have the
ability to input entry and exit records into the data base
and to make queries.

If immigration databases are available at some POEs, but not
all, how does the host government decide which POEs will
receive the tool?

Some isolated seaports with low vessel traffic do not have
connectivity to the JIB mainframe.

-- What problems, if any, limit the effectiveness of the
systems? For example, limited training, power brownouts,
budgetary restraints, corruption, etc.?

Computer systems and equipment used by the Immigration Bureau
are modern and efficient. The limitations of the computer
systems are not technological; they are self-imposed
restrictions on cooperation with other agencies within Japan
and with foreign immigration authorities. Corruption within
the Immigration Bureau is not a concern.

-- How often are national immigration databases updated?

Records of immigration entries and exits are updated
immediately. Watchlists maintained by JIB and available at
the ports of entry are updated within 10 minutes of input.

-- What are the country's policies (legislation, mandates,
etc.) on collecting information from travelers arriving in

the country?

In addition to biographical information on the passport, Japan (since November 2007) collects biometric information (facial photograph and digital scans of both index fingers) from all foreigners arriving at air and sea ports. Diplomats, certain permanent residents, and U.S. military members entering Japan under the Status of Forces Agreement are exempt from providing biometrics.

-- Are there different policies for entry and exit at air, sea, and land POEs and for domestic flights?

Policies for entry and exit at air and sea ports are the same. Passengers on domestic flights are not required to provide any identification at check in or prior to boarding.

-- What agency oversees the collection of traveler information?

Immigration Bureau collects and manages all information on travelers.

-- What are the policies of the collecting agency to share that information with foreign governments?

The Immigration Bureau has legal authority to share information internationally with only other Immigration authorities.

-- Does the host government collect Passenger Name Record (PNR) data on incoming commercial flights or vessels? Is

this data used for intelligence or law enforcement purposes to screen travelers in a systematic way? Does host government have any existing treaties to share PNR data?

The Immigration Bureau has access to PNR data on incoming commercial flights and uses this data in conjunction with API data to screen travelers. The government does not have a treaty to share PNR data with the U.S.

-- If applicable, have advance passenger informationsystems (APIS), interactive advanced passenger information systems (IAPIS), or electronic travel authority systems been effective at detecting other national security threats, such as wanted criminals?

The Immigration Bureau initiated APIS on January 4,2005, as a voluntary program. Under APIS, airlines and ships are required to report passenger and crew manifests (names and certain identifying information) in advance of arrival. As a voluntary program, only about 30% of air carriers provided passenger manifest information. Effective February 1,2007, APIS reporting for flights inbound to Japan was made mandatory (as a result of the May 24,2006 revisions to the Immigration Control Act). There is no requirement to report passenger information on flights outbound from Japan. It is also not a requirement to submit the manifest information electronically although nearly all carriers do. Carriers must submit passenger manifests 90 minutes prior to arrival of the aircraft to a joint Immigration and Customs computer server. The server is managed by the Immigration Bureau. Manifest information is run electronically against the Blacklist and Nyushin List (Entry Refusal List). Police officers will respond to any Blacklist matches. Immigration will refuse entry to Nyushin (Entry Refusal List) matches. Japan Customs electronically runs the APIS data against its own Watchlist.

¶2. (SBU) Watchlisting:

Is there a name-based watchlist system used to screen travelers at POEs? What domestic sources of information populate the name-based watchlist, i.e. names of deported persons, terrorist lookouts, criminal wantslwarrants? If host

government maintains a watchlist, how many records does the watchlist contain, and how many are terrorist-related? -- Which ministry or ofice maintains the watchlist?

-- What international watchlists do the host government use for screening individuals, e.g. Interpol or TSA No Fly lists, UN, etc.?-- What bilaterdmultilateral watchlist agreements exist between host government and its neighbors?

The Immigration Bureau maintains 3 Watchlists for entry control purposes. All 3 Watchlists are available at the ports of entry that handle regularly scheduled airline flights. The Watchlists are updated within 10 minutes of new input. The first Watchlist is called the Blacklist. It consists of biographical information on known and suspected terrorists, members of domestic terrorist organizations (Japan Red Army), identifications received from foreign law enforcement and intelligence agencies, Japanese police wanted persons, and InterPOL wanted persons. The Blacklist also contains fingerprints of known and suspected terrorists obtained from InterPOL, pictures and fingerprints of previously deported foreign nationals, and figerprints of wanted persons. The second Watchlist is called the Nyushin List (entry refusal list) which consists of non-criminal information related to eligibility for admission. The Nyushin List contains previous immigration violators (primarily deportees and overstays) who are barred from re-entering Japan. It also contains some overlap with Blacklist information. The third Watchlist is the Youchui List (Lookout list) which consists of suspected violators, possible matches, and warnings. These 3 Watchlists total about 600,000 records.

Ports of entry have read only access to the Watchlists. Only the Narita Airport Data Center has the ability to add or delete names from the lists. Ports of entry have to send additions and deletions to the list to Narita. The Watchlists match at entry and exit against exact names and similar names based on common alphabet characters (e.g. Mohammad, Muhamid). Other agencies within Japan can add names to the lists but must make the request in writing to Immigration Bureau Headquarters. Approved requests are sent to the Narita Airport Data center for input.

¶3. (SBU) Biometrics:

-- Are biometric systems in place at ports of entry (air, land, sea)? If no, does host government have plans to install such a system? If biometric systems are available at some POEs, but not all, how does the host government decide what POEs will receive the tool?

Yes

-- What biometric technologies, if any, does the host government use, i.e. fingerprint identification, facial recognition, iris recognition, hand geometry, retinal identification, DNA-based identification, keystroke dynamics, gait analysis? Are the systems ICAO compliant?

Under the amended Immigration Control Act, which entered into force on November 20,2007, foreign nationals (excluding diplomats, SOFA personnel, special permanent residents, and those under 16 years of age) are required to provide electronic scans of both index fingers and a facial photo as part of entry inspection. The system is similar to the US-VISIT system.

-- Are biometric systems integrated for all active POEs? What are the systems and models used? Are all passengers screened for the biometric or does the host government target a specific population for collection (i.e. host country nationals)? Do the biometric collection systems look for a one to one comparison (ensure the biometric presented matches the one stored on the e- Passport) or one to many comparisons (checking the biometric presented against a

database of known biometrics)?

The biometric collection system is in place at all active ports of entry. Japanese nationals and certain foreign nationals are excluded from the requirement to provide biometrics. Finger scans are electronically registered and matched against a data base of fingerprints of previous deportees to prevent terrorists and those previously deported from entering under new identities.

-- If biometric systems are in place, does the host government know of any countermeasures that have been used or attempted to defeat biometric checkpoints?

During January 2009, a Korean female generated significant press interest by claiming that she had spoofed the Japan biometric system and was able to re- enter Japan after being deported by applying a special tape over her fingers. The tape allegedly changed her prints such that she was not detected at entry. The Immigration Bureau investigated and the results were inconclusive; however, as a result of that incident, Immigration Inspectors have been instructed to pay closer attention to passengers to ensure their fingers are not covered with tape. The Immigration Bureau is also working with the manufacturer to enhance the equipment's capability to detect unnatural prints.

-- What are the host government's policies on collecting the fingerprints of travelers coming into the country?

All foreign nationals (excluding diplomats, SOFA personnel, special permanent residents, and those under 16 years of age) are required to provide electronic scans of both index fingers and a facial photo as part of entry inspection.
-- Which agency is responsible for the host government's fingerprint system?

Immigration Bureau

-- Are the fingerprint programs in place NIST, INT-I, EFTS, UKl or RTID compliant?

Unknown

-- Are the fingerprints collected as flats or rolled? Which agency collects the fingerprints?

Prints are flat. Immigration Bureau collects the prints.

¶4. (SBU) Border Control and Screening:

-- Does the host government employ software to screen travelers of security interest?

Biographical data from passports is matched against computerized watchlists to detect persons who may be of security interest.

-- Are all travelers tracked electronically, or only non-host- country nationals? What is the frequency of travelers being "waived through" because they hold up what appears to be an appropriate document, but whose information is not actually recorded electronically?

Entry and exit information is kept for both Japanese and foreign country nationals. Travelers are not "waived through". All travelers must go through immigration inspection. In order to speed up immigration procedures, Japan Immigration introduced automated gates on November 20,2007. Japanese nationals who have had their biographical information and fingerprints registered in advance or foreign nationals who meet certain requirements (having a reentry permit, registered fingerprints and facial photograph) may bypass inspection by immigration officers. What is the estimated percentage of non-recorded crossings, entries and exits? Extremely low. Among the foreign

nationals deported during 2007, there were 342 found to have entered Japan without inspection. 9,152,186 foreign nationals entered Japan during 2007. 34219,152,186 = 0.003%.

-- Do host government border control officials have the authority to use other criminal data when making decisions on who can enter the country? If so, please describe this authority (legislation, mandates, etc).

Immigration Bureau can deny entry to foreigners with criminal histories. If the Immigration Bureau has reason to believe a foreigner has a criminal history, the Immigration Bureau may request the criminal history details from the foreigner's home country and use that information as part of the entry decision process.

-- What are the host government's policies on questioning, detaining and denying entry to individuals presenting themselves at a point of entry into the country? Which agency would question, detain, or deny entry?

Immigration Bureau has authority to make entry decisions. By process, Immigration Inspectors in the primary inspection booths receive "hit" notification but no details. Hits are handled in secondary inspection where detailed information resulting in the hit is available. The purpose is to expedite primary processing. Immigration Bureau's goal is to get the passenger from aircraft exit to completion of primary processing in 20 minutes. Immigration Inspectors have authority to question, detain, and deny entry. Criminal arrests must be made by the Police.

-- How well does information sharing function within the host government, i.e., if there is a determination that someone with a valid host-government visa is later identified with terrorism, how is this communicated and resolved internally?

Japan's bureaucracy is famously stovepiped. As a result, there is no unified government-wide terrorism watchlist. Immigration, Customs, Police, and the Public Security Intelligence Agency maintain separate lists.

¶5. (SBU) Passports:

-- Does the host government issue a machine-readable passport containing biometric information? If so, what biometric information is included on the document, i.e. fingerprint, iris, facial recognition, etc.? If not, does host government plan to issue a biometric document in the future? When?

Yes. The biometric information is mainly facial recognition, ie. a photograph.

-- If the host government issues a machine-readable passport containing biometric information, does the host government share the public key required to read the biometric information with any other governments? If so, which governments? Does the host government issue replacement passports for full or limited validity (i.e. the time remaining on the original passports, fixed validity for a replacement, etc.)?

The Government of Japan does share the public key required to read the biometric information. Unknown if they share this with other governments. Replacement passports are issued as full validity. They are considered new passports. Temporary passports are issued for one year validity or one trip back to Japan "emergency passports" depending on circumstances.

-- Does the host government have special regulations/procedures for dealing with "habitual" losers of passports or bearers who have reported their passports stolen multiple times?

It is more difficult for persons who are "habitual" losers of passports to obtain new passports, but similar to the USG, it is not impossible. When a person who is a "habitual" loser of passports applies for a new passport, it is identified through a namecheck procedure and they undergo more rigorous questioning. -- Are replacement passports of the same or different appearance and page length as regular passports (do they have something along the lines of our emergency partial duration passports)?

Replacement passports are of the same appearance, except for the "return to Japan" emergency travel documents. -- Do emergency replacement passports contain the same or fewer biometric fields as regular-issue passports?

Emergency replacement travel documents contain a facial biometric with a photograph, but they are not/not e-passports. Replacement passports are regular issue passports and as such they contain the same biometric fields. -- Where applicable, has Post noticed any increase in the number of replacement or "clean" (i.e. no evidence of prior travel) passports used to apply for U.S. visas?

No,.

-- Are replacement passports assigned a characteristic number series or otherwise identified?

No.

¶6. (SBU) Fraud Detection:

-- How robust is fraud detection and how actively are instances of fraud involving documents followed up?

There are very few instances of fraud. Fraud is reported to the local police, who investigate according to need.

-- How are potentially fraudulently issued documents taken out of circulation, or made harder to use?

Potentially fraudulent documents are not removed out of circulation. Fraudulent documents are removed out of circulation.

¶7. (SBU) Privacy and Data Security:

-- What are the country's policies on records related to the questioning, detention or removal of individuals encountered at points of entry into the country? How are those records stored, and for how long?

The vast majority of immigration encounters occur at ports of entry. It is unknown how those records are stored or for how long.

-- What are the country's restrictions on the collection or use of sensitive data?

The Immigration Bureau protects personal identification information through a combination of encryption and access restriction. Personal identification information is encrypted and transmitted between server centers and desktop clients on a "closed network" via leased communication lines. User access to the system is by biometric authentication.

-- What are the requirements to provide notice to the public on the implementation of new databases of records?

Unknown, but likely to be stringent. Privacy laws in Japan are robust and very narrowly interpreted.

-- Are there any laws relating to security features for government computer systems that hold personally identifying information?

Unknown, but it is highly likely there are laws relating to

security features for government computer systems. -- What are the rules on an individual's ability to access data that homeland security agencies hold about them?

Unknown

-- Are there different rules for raw data (name, date of birth, etc.) versus case files (for example, records about enforcement actions)?

Unknown

-- Does a non-citizen resident have the right to sue the government to obtain these types of data?

Unknown.

¶8. (SBU) Identifying Appropriate Partners: Department would appreciate post's in-house assessment of whether host government would be an appropriate partner in data sharing. Considerations include whether host government watchlists may include political dissidents (as opposed or in addition to terrorists), and whether host governments would share or use U.S. watchlist data inappropriately, etc.

-- Are there political realities which would preclude a country from entering into a formal data-sharing agreement with the U.S.?

Privacy laws are very strictly interpreted. Ministries are highly stove- piped and do not share information with each other, or even within bureaus of the same Ministry.

-- Is the host country's legal system sufficiently developed to adequately provide safeguards for the protection and nondisclosure of information?

Yes, but it is a question of developing the political will to pass legislation which would allow data- sharing including safeguards for the protection of nondisclosure. There are concerns that Japan does not have system and a means to protect classified information.

-- How much information sharing does the host country do internally? Is there a single consolidated database, for example? If not, do different ministries share information amongst themselves?

Very little information is shared internally. There is no/no consolidated terrorist screening database. Ministries do not willingly share information among themselves. Some sharing does occur.

-- How does the country define terrorism? Are there legal statutes that do so?

Unknown.
ZUMWALT